

AddAccess-ACE

Access Control Entries not inheritable

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2005 Cigital, Inc.

2005-10-03

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4395 bytes

Attack Category	<ul style="list-style-type: none">Privilege Exploitation						
Vulnerability Category	<ul style="list-style-type: none">Access Control						
Software Context	<ul style="list-style-type: none">Security						
Location	<ul style="list-style-type: none">winbase.h						
Description	<p>When an access control entry (ACE) is added via <code>AddAccessAllowedAce()</code> or <code>AddAccessDeniedAce()</code>, this entry is not inheritable, which can create a vulnerability to attack if inheritance is assumed.</p> <p>The <code>AddAccessAllowedAce</code> function adds an access-allowed ACE to an access control list (ACL). The access is granted to a specified security identifier (SID).</p> <p>The <code>AddAccessDeniedAce</code> function adds an access-denied ACE to an ACL. The access is denied to an SID.</p> <p>The ACE added by <code>AddAccessDeniedAce</code> is not inheritable. This can lead to subclasses not being denied access when they should be.</p>						
APIs	<table><tr><th>FunctionName</th><th>Comments</th></tr><tr><td><code>AddAccessAllowedAce</code></td><td></td></tr><tr><td><code>AddAccessDeniedAce</code></td><td></td></tr></table>	FunctionName	Comments	<code>AddAccessAllowedAce</code>		<code>AddAccessDeniedAce</code>	
FunctionName	Comments						
<code>AddAccessAllowedAce</code>							
<code>AddAccessDeniedAce</code>							
Method of Attack	<p>If <code>AddAccessDeniedAce</code> is used to restrict access to an object, then the access restriction will not propagate any child objects. If the restriction should have been propagated to the children, then</p>						

1. <http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html> (Barnum, Sean)

	access rights for the children will be more permissive than was intended, and an attacker could exploit this.		
Exception Criteria			
Solutions	Solution Applicability	Solution Description	Solution Efficacy
	Whenever adding an ACE.	To control whether the new ACE can be inherited by child objects, use the AddAccessAllowedAceEx or AddAccessDeniedAceEx function.	Effective, given appropriate thought as to proper access permissions.
Signature Details	BOOL AddAccessAllowedAce(PACL pAcl,DWORD dwAceRevision,DWORD AccessMask,PSID pSid); BOOL AddAccessDeniedAce(PACL pAcl,DWORD dwAceRevision,DWORD AccessMask,PSID pSid);		
Examples of Incorrect Code	<pre>if (! AddAccessDeniedAce(pAcl, dwAceRevision, AccessMask, pSid) { /* handle error */ }</pre>		
Examples of Corrected Code	<pre>DWORD AceFlags = OBJECT_INHERIT_ACE; // Inheritance flags should be set as appropriate if (! AddAccessDeniedAceEx(pAcl, dwAceRevision, AceFlags, AccessMask, pSid) { /* handle error */ }</pre>		
Source Reference	<ul style="list-style-type: none"> Howard, Michael & LeBlanc, David C. <i>Writing Secure</i> 		

	Code, 2nd ed. Redmond, WA: Microsoft Press, 2002, ISBN: 0735617228., p.409	
Recommended Resources	<ul style="list-style-type: none"> • MSDN reference for AddAccessAllowedAce² • MSDN reference for AddAccessDeniedAce³ 	
Discriminant Set	Operating System	<ul style="list-style-type: none"> • Windows
	Languages	<ul style="list-style-type: none"> • C • C++

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. <mailto:copyright@cigital.com>